Express Mail Label No. **HAND DELIVERED**

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
YOR9-2000-0385US1
Total Pages in this Submission

TO THE ASSISTANT COMMISSIONER FOR PATENTS
Box Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

ACCESS CONTROL FOR RENTAL CARS

and invented by:

Te-Kai Liu and Michael C. Greenwood

If a CONTINUATION APPLICATION, *check appropriate box and supply the requisite information:*

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having **14** pages and including the following:
   - a. ☒ Descriptive Title of the Invention
   - b. ☐ Cross References to Related Applications *(if applicable)*
   - c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*
   - d. ☐ Reference to Microfiche Appendix *(if applicable)*
   - e. ☒ Background of the Invention
   - f. ☒ Brief Summary of the Invention
   - g. ☒ Brief Description of the Drawings *(if drawings filed)*
   - h. ☒ Detailed Description
   - i. ☒ Claim(s) as Classified Below
   - j. ☒ Abstract of the Disclosure

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No. YOR9-2000-0385US1
Total Pages in this Submission

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*
   a. ☐ Formal Number of Sheets _____
   b. ☒ Informal Number of Sheets 6
4. ☒ Oath or Declaration
   a. ☒ Newly executed *(original or copy)* ☐ Unexecuted
   b. ☐ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*
   c. ☒ With Power of Attorney ☐ Without Power of Attorney
   d. ☐ *DELETION OF INVENTOR(S)*
   Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ Computer Program in Microfiche *(Appendix)*
7. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*
   a. ☐ Paper Copy
   b. ☐ Computer Readable Copy *(identical to computer copy)*
   c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. ☒ Assignment Papers *(cover sheet & document(s))*
9. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*
10. ☐ English Translation Document *(if applicable)*
11. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Acknowledgment postcard
14. ☐ Certificate of Mailing
    ☐ First Class ☐ Express Mail *(Specify Label No.):* **HAND DELIVERED**

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
YOR9-2000-0385US1
Total Pages in this Submission

Accompanying Application Parts (Continued)

15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*

16. ☐ Additional Enclosures *(please identify below):*

Fee Calculation and Transmittal

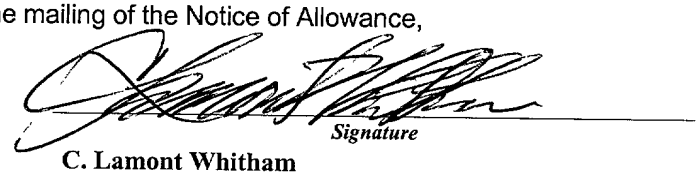
CLAIMS AS FILED

For	#Filed	#Allowed	#Extra		Rate	Fee
Total Claims	19	- 20 =	0	x	$18.00	$0.00
Indep. Claims	2	- 3 =	0	x	$78.00	$0.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
					BASIC FEE	$690.00
OTHER FEE *(specify purpose)*						$0.00
					TOTAL FILING FEE	$690.00

☐ A check in the amount of to cover the filing fee is enclosed.

☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. **50-0510/IBM** as described below. A duplicate copy of this sheet is enclosed.

- ☒ Charge the amount of **$690.00** as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).



Signature

Dated: **August 31, 2000**

C. Lamont Whitham
Reg. No. 22,424

McGuireWoods LLP
1750 Tysons Boulevard, Suite 1800
McLean, VA 22102
(703)712-5000

cc:

LAW OFFICES
McGuireWoods LLP
1750 TYSONS BOULEVARD, SUITE 1800
MCLEAN, VIRGINIA 22102

09/15/2000 09:54:05

APPLICATION FOR UNITED STATES LETTERS PATENT

Applicants: Te-Kai Liu and Michael C. Greenwood
For: ACCESS CONTROL FOR RENTAL CARS
Docket No.: YOR9-2000-0385US1

ACCESS CONTROL FOR RENTAL CARS

DESCRIPTION

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention generally relates to a car rental system and, more particularly, to a car rental system in which cars are operated by digital keys instead of conventional metal keys.

Background Description

In a typical car rental system today, car keys are left in cars when cars are waiting to be picked up by customers or when cars are dropped off by customers at a gated parking lot. Consequently, keys are vulnerable to be stolen or copied. It is very costly to disable a stolen key-usually an authorized car dealer or locksmith needs to be involved. It is also very dangerous when a car key is copied by a malicious person who can follow the car when it exits the parking lot, and steal the car when it is unattended.

U.S. Patent Nos. 5,289,369 to Hirshberg and 5,812,070 to Tagami et al. disclose integrated circuit (IC) card based access control methods where each car is equipped with a IC card reader which can communicate with a cental station by wireless communications. The cards in these patents store the identifications (IDs) of the renters carrying the cards. Upon being inserted into a card reader on a rental car, the ID stored in the card is read out and sent to the cental station to check for proper authorization. In case of outage of

wireless communications, the system will fail to work.

U.S. Patent No. 4,477,874 to Ikuta et al. discloses an off-line access control method based on the secret codes stored on a car and a card. Basically, a car stores two secret codes, one for master and the other for slave. A card that carries the master secret has full control of the car, whereas the card carrying the slave secret code has limited control. For example, a slave card only authorizes the driver to start the engine but not to open the trunk lid. In such a system, if the master card is lost, the car reader has to be re-programmed with a new master secret code. This system is not suitable for a rental system since the reader on the car needs to be re-programmed for every renter.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a car rental system which does not use conventional metal car keys.

It is another object of the invention to provide a car rental system where network connection from cars to a central station is not required to check whether a renter has the proper authorization to operate a car.

It is yet another object of the invention to provide a car rental system where there is no pre-processing to be done on the car to be rented for every rental transaction.

According to the invention, the cars of the car rental system can be made operable by having a renter present a digital key issued from the car rental system. The digital key specifies the starting date and time of a given rental transaction, and the identification of the car the key is for. The digital key is further signed by the car rental system for authenticity. The way a digital key gets into a renter's hand is as follows. A prospective renter makes online reservation over the Web (i.e., the World Wide Web portion of the

Internet) and downloads into a portable storage device a digital key which can be used to operate the reserved car on the day the reservation is made for. On the pickup day, the renter goes to the car and inserts the portable storage device into a slot on the car. Upon successful verification of the digital key, the car is enabled and the renter can keep the car until he or she wants to return the car. The return process starts by having the renter obtain a invalidated digital key from the car. Once the rental car invalidates the digital key provided by the renter, the renter can no longer operate the rental car. Since the in-car controller is able to decipher the given authorization information, there is no need to re-program the in-car controller for each renter.

According to another aspect of the invention, the renter will be held liable for the rental car until he or she presents the invalidated digital key to the central station of the car rental system. To facilitate this, the car rental system will set up kiosks with readers to interface with the portable storage carried by the renters. The kiosks can be stationary which have a wired network connection to the cental station of the car rental system, or they can be mobile (e.g., located on a trailer, a van, a truck) which have a wireless network connection to the cental station.

To prevent a lost digital key from being used by unauthorized parties, a digital key can contain information such as a personal identification number (PIN) or a hash of the PIN of the authorized renter. For extra protection, the renter can opt to include his or her PIN in the digital key when the key is created by the car rental system.

The parking lot of the car rental system according to the invention can be operated without security personnel checking for proper authorization, hence saving labor cost and eliminating human efforts. With this advantage, the car rental system can open up more satellite rental sites which can operate around the clock. This would dramatically improve the service offering to the

renters and in turn encourage more rental opportunities.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

Figure 1 is a block diagram showing the basic components of the car rental system;

Figure 2 is a flow diagram for the reservation process;

Figure 3 is a block diagram of the in-car access control system;

Figure 4 is a flow diagram for the verification process implemented on the cars;

Figure 5 is a flow diagram for the car return process implemented on the cars; and

Figure 6 is a flow diagram for the car return process implemented on a kiosk.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT OF THE INVENTION

Referring now to the drawings, and more particularly to Figure 1, there is shown a block diagram illustrating the basic components of the invention. These include a computing system 10, a portable storage device 12, and an access control device 14 with a interface 16 to a portable storage inside a rental car 160.

The computing system 10 is used to make a reservation according to the needs of the renter. The computing system is also used to create and store digital keys for access to a rental car. The computing system may be located

within a kiosk 140 at a car rental agency. The computing system may be a simple terminal connected through a network (i.e., an intranet or the Internet) 120 to a central reservation server 110 which accepts reservation requests, checks the availability of cars, and creates digital keys for access to the reserved cars. Alternatively, a personal computer (PC) 130 located at the home, office or other location may be used as a terminal to connect to the central reservation server 110. Either the computing system in the kiosk or the PC may be provided with means to download digital keys to a portable storage device 12.

The portable storage device is preferably a smart card issued by a car rental agency. Other memory devices may be used such as, for example, a Personal Digital Assistant (PDA), a memory card (such as the Personal Computer Memory Card International Association (PCMCIA) card), or a diskette. The manner in which a digital key is downloaded is entirely conventional.

In the case of a smart card, the renter then carries the smart card 12 to the car which contains a access control device 14. The card is inserted into the reader slot to provide the access control device 14 with the digital key generated by the computing system 10. The access control device 14 then makes decision on whether or not to give the card holder access to the car, according to the date and time and car ID information in the digital key.

Figure 2 is a flow diagram showing the reservation process executed by the reservation server 110. The reservation server 110 in the first step 202 authenticates the user visiting the reservation Web site. Upon the reservation server successfully authenticating the user (either by name and password or by a security token such as a smart card), the user is prompted for the date, time, and location for pickup and return, and the type of car in step 204. Upon the user submitting the request, the reservation server receives and processes the request in step 206. The server 110 checks the availability in step 208. If a

suitable car is not available, the user is prompted to file a reservation request again in step 204. If there is a car available, the server 110 starts to create a digital key in steps 210 to 216. Specifically, the server 110 obtains car and user information (e.g., car ID and user's PIN) in step 210. The server 110 computes the hash of user's PIN in step 212. The server 110 combines car and user information with the hashed PIN in step 214. The server 110 digitally signs the combined information using the private key of the reservation server 110 in step 216. The server then responds to the user with a Web page where a hyperlink points to the signed information (i.e., digital key) in step 218. Finally the user downloads the signed information and saves it into a portable storage device 12 in step 220.

Figure 3 is a block diagram for the in-car access control system. The system includes an access controller 330, an electronic control unit 320, and actuators 310. The access controller 330 on one hand is connected to a smart card slot 342 for accepting user's smart card 12, a keypad for accepting user's PIN, and an output device such as light emitting diodes (LEDs) for signaling an error to the user. The access controller 330 on the other hand interfaces with a electronic control unit (ECU) 320 which is connected to actuators 310 in charge of actuating various in-car instruments such as doors 302, engine 304, and trunk lid 306.

Figure 4 is a flow diagram for the in-car access controller 330. Upon detecting a smart card inserted into the smart card slot 16, the access controller 330 obtains the digital key stored on the smart card in step 402. The access controller 330 checks whether the digital key is already invalidated in step 404. If so, the access controller 330 signals an error to the smart card holder in step 420. If the digital key is not invalidated yet, the access controller 330 verifies the signature on the digital key in step 406. If the signature is not an authentic one from the reservation server 110, the card holder is signaled an error in step 420. If the signature is genuine in step 408, the user is prompted

for PIN in step 410. The controller then checks for correctness of the PIN in step 412. If the input PIN matches the one in the smart card, the access controller 330 activates the instruments which the user are authorized to have access to in step 414. If the input PIN is incorrect in step 412, the user is prompted again for the correct PIN. If the input PIN fails to match for three trials in step 416, the access controller 330 invalidates the digital key in step 418 by making a record in its storage device.

Figure 5 shows a flow diagram for the in-car access controller 330 upon receiving the renter's request to return the car. The user is prompted for inserting his or her smart card into the smart card slot in step 502 if not already done so. The access controller 330 obtains car status information such as fuel level, mileage, current time and car ID from the ECU 320 in step 504. The access controller proceeds to create a return packet by combining car status information and the current digital key in step 506. It then signs the return packet using the private key of the car in step 508. The access controller 330 appends the car ID to the signed return packet in step 510. It then saves the signed return packet into the smart card in step 512. Finally, the access controller 330 invalidates the current digital key in step 514 by making a record in its storage device.

Figure 6 shows a flow diagram for the kiosk 140 upon receiving renter's request to return the car. The kiosk 140 first prompts the user to insert his or her smart card in step 602. The kiosk 140 tries to retrieve the return packet from the smart card in step 604. If the return packet is not found in step 606, the user is notified to get the return packet from the car first in step 616. If the return packet is present, the kiosk verifies the signature on the return packet in step 608. If the signature is not found to be an authentic one from the car to be returned in step 610, the user is advised to contact customer service for assistance in step 618. If the signature is found to be genuine in step 610, the kiosk 140 updates the car status stored at the reservation server 110 in step

612. The kiosk 140 finally prints a receipt for the user in step 614.

While the invention has been described in terms of a single preferred embodiment, those skilled in the art will recognize that the invention can be practiced with modification within the spirit and scope of the appended claims.

9959259 "959259

CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

1. A car rental system comprising:

a fleet of cars, each of which is operable only when a valid digital key is presented to the car, and each of said fleet of cars has a means to invalidate a digital key; and

a management system for handling reservation and car return, said management system including:

a key generation system for generating digital keys for renters of the car rental system;

a key return system for processing digital keys returned by renters.

2. The system in claim 1, further comprising a parking lot guarded by a security gate, said fleet of cars being parked with confines of said parking lot when not rented by a renter of the car rental system, said security gate only opening when a valid digital pass is presented by a renter of the car rental system.

3. The system in claim 1, wherein the management system is accessed by a prospective renter over a network and the prospective renter is given a digital key to operate a particular car and a digital pass to open the gate of the parking lot where said particular car is parked, after said prospective renter completes a reservation for said particular car, said digital key and digital pass being effective starting from the time specified by said reservation.

4. The system in claim 3, wherein the prospective renter accesses the management system at a kiosk located in the parking lot where the particular car is parked.

5. The system in claim 3, wherein the prospective renter accesses the management system over the Internet.

6. The system in claim 3, wherein the key generation system stores a digital key on a storage device provided by a prospective renter.

7. The system in claim 6, wherein the storage device is a smart card.

8. The system in claim 6, wherein the digital key comprises car and user identification (ID) signed by the management system to authenticate the digital key.

9. The system in claim 1, wherein a renter of a car invalidates a valid digital key upon returning a car to the car rental system and presents an invalidated digital key to the key return system to complete a car return.

10. The system in claim 9, wherein the invalidation of a valid digital key includes storing car status information relevant to computing by the key return system a receipt for the renter.

11 . A computer implemented method for operating a car rental system comprising the steps of:

accessing a reservation server by a prospective car renter to reserve a car;

authenticating the prospective car renter by the reservation server and,

upon the reservation server successfully authenticating the user, prompting the prospective car renter for the date, time, and location for pickup and return, and the type of car;

checking by the reservation server an availability of a requested car and, if a car is available, creating by the reservation server a digital key by car and user information with a digital signature of the reservation server; and

downloading the digital key to a portable storage device, the portable storage device being used to gain access to a rental car.

12. The method in claim 11, wherein the step of accessing the reservation server is performed via a network.

13. The method in claim 12, wherein the network is the Internet.

14. The method in claim 11, wherein the step of authenticating a prospective car renter includes the steps of:

prompting the prospective car renter to enter a personal identification number (PIN); and

comparing the entered PIN with a valid PIN for the prospective car renter.

15. The method of claim 11, wherein the step of creating a digital key comprises the steps of:

computing a hash of the car renter's valid PIN;

combining car and renter identification with the hashed PIN; and

digitally signing the combined information by said reservation server.

16. The method in claim 11, further comprising the steps of:

inserting the portable storage device by a car renter into a slot for

receiving the portable storage device in a rented car;

upon detecting the portable storage device inserted into the slot, obtaining by an access controller installed in the rented car the digital key stored on the portable storage device and checking by the access controller whether the digital key is valid and verifying the signature on the digital key;

if the digital key is valid and the signature is verified, the access controller then prompting the car renter to enter his or her identification and checking for correctness of the car renter's identification; and

if the entered identification for the car renter matches a correct identification on the portable storage device, the access controller activating instruments of the car which the car renter is authorized to have access to.

17. The method in claim 16, further comprising the steps of:

upon receiving a car renter's request to return a car, prompting the car renter to insert his or her portable storage device into the slot for the portable storage device;

obtaining by the access controller car status information and car identification;

creating by the access controller a return packet by combining car status information and the current digital key;

signing the return packet by the access controller, appending the car identification to the signed return packet, and saving the signed return packet into the portable storage device; and

invalidating by the access controller a current digital key.

18. The method in claim 17, further comprising the steps of:

upon receiving a car renter's request to return a car, retrieving the return packet from the portable storage device;

verifying a signature on the return packet; and

updating the car status and printing a receipt for the car renter.

19. The method in claim 11, wherein the portable storage device is a smart card.

09525605 . 062700

ACCESS CONTROL FOR RENTAL CARS

ABSTRACT OF THE DISCLOSURE

Cars of a car rental system are made operable by having a renter present a digital key issued from the car rental system. The digital key specifies the starting date and time of a given rental transaction, and the identification of the car the key is for. The digital key is further signed by the car rental system for authenticity. A prospective renter makes online reservation over the Web and downloads into a portable storage device a digital key which can be used to operate the reserved car on the day the reservation is made for. On the pickup day, the renter goes to the car and inserts the portable storage device into a slot on the car. Upon successful verification of the digital key, the car is enabled and the renter can keep the car until he or she wants to return the car. The return process starts by having the renter obtain a invalidated digital key from the car. Once the rental car invalidates the digital key provided by the renter, the renter can no longer operate the rental car. Since the in-car controller is able to decipher the given authorization information, there is no need to re-program the in-car controller for each renter. The renter will be held liable for the rental car until he or she presents the invalidated digital key to the central station of the car rental system. To prevent a lost digital key from being used by unauthorized parties, a digital key can contain information such as a personal identification number (PIN) or a hash of the PIN of the authorized renter. For extra protection, the renter can opt to include his or her PIN in the digital key when the key is created by the car rental system. The parking lot of the car rental system can be operated without security personnel checking for proper authorization.

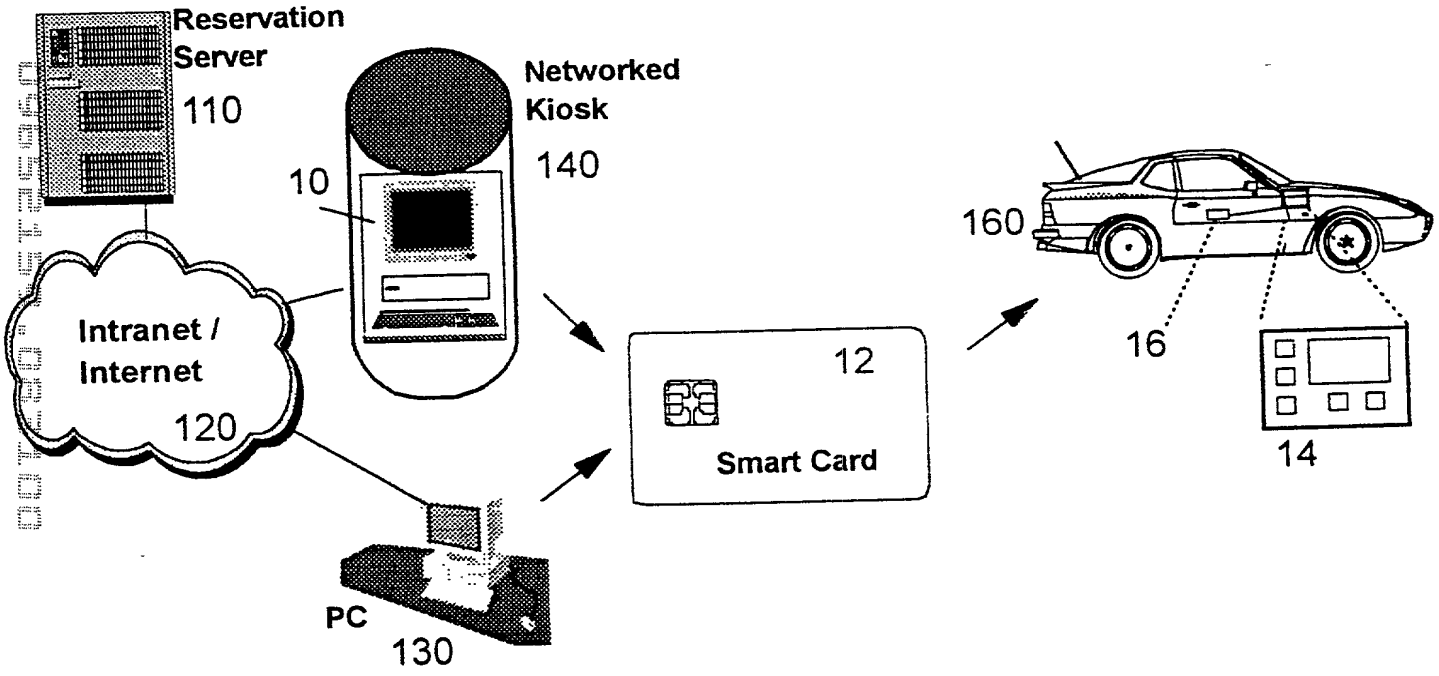

Reservation
Server
110
Networked
Kiosk
140
10
Intranet /
Internet
120
12
Smart Card
160
16
14
PC
130

Figure 1

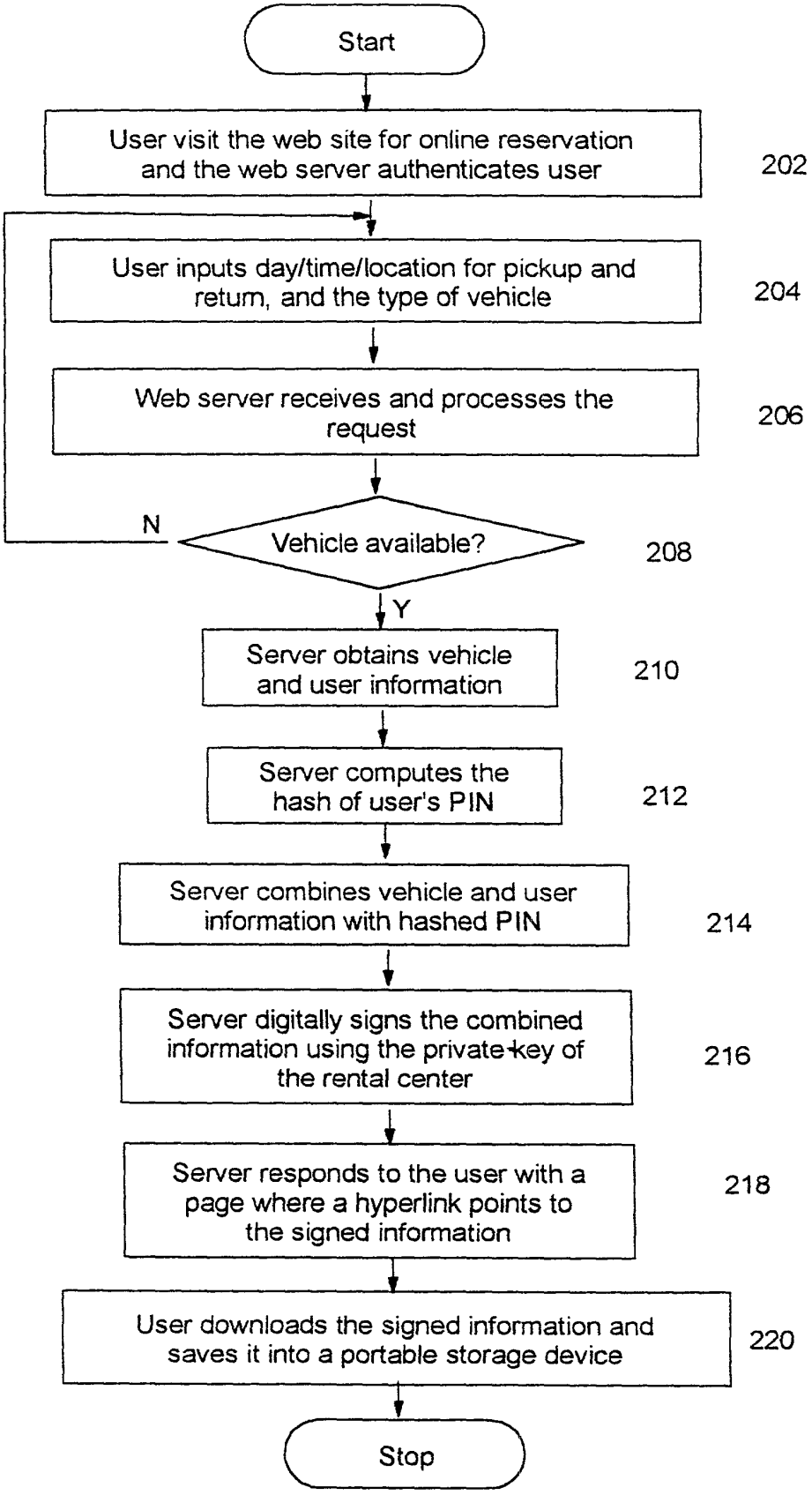

Start
User visit the web site for online reservation and the web server authenticates user
202
User inputs day/time/location for pickup and return, and the type of vehicle
204
Web server receives and processes the request
206
N
Vehicle available?
208
Y
Server obtains vehicle and user information
210
Server computes the hash of user's PIN
212
Server combines vehicle and user information with hashed PIN
214
Server digitally signs the combined information using the private key of the rental center
216
Server responds to the user with a page where a hyperlink points to the signed information
218
User downloads the signed information and saves it into a portable storage device
220
Stop

Figure 2

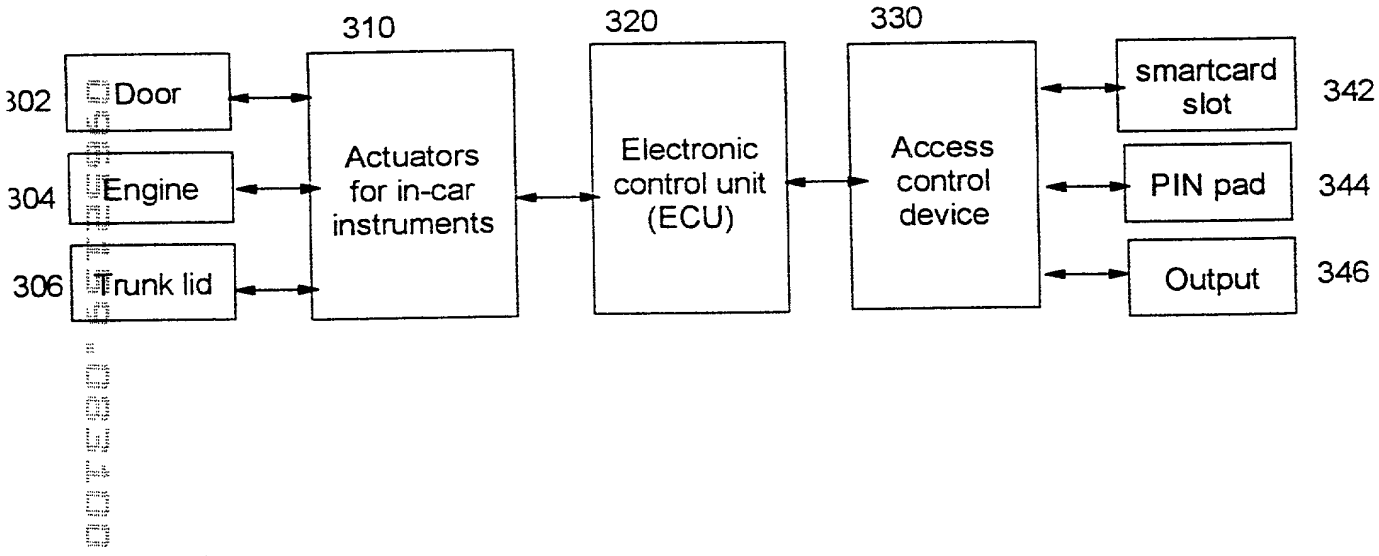

310
320
330
302
Door
304
Engine
306
Trunk lid
Actuators for in-car instruments
Electronic control unit (ECU)
Access control device
smartcard slot
342
PIN pad
344
Output
346

Figure 3

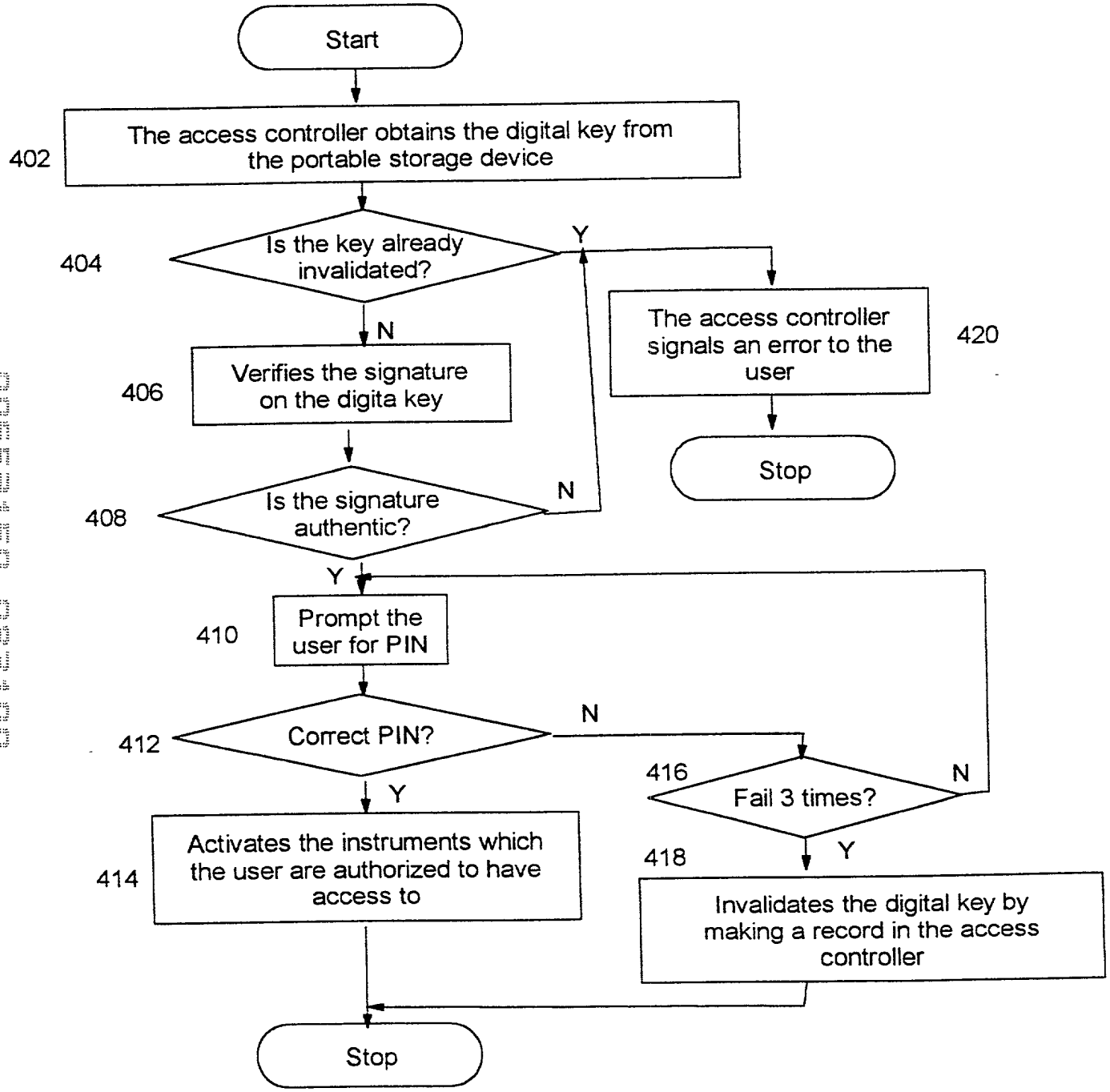

Start
The access controller obtains the digital key from the portable storage device
402
Is the key already invalidated?
404
Y
N
The access controller signals an error to the user
420
Stop
Verifies the signature on the digita key
406
Is the signature authentic?
408
N
Y
Prompt the user for PIN
410
Correct PIN?
412
N
Y
Fail 3 times?
416
N
Y
Activates the instruments which the user are authorized to have access to
414
Invalidates the digital key by making a record in the access controller
418
Stop

Figure 4

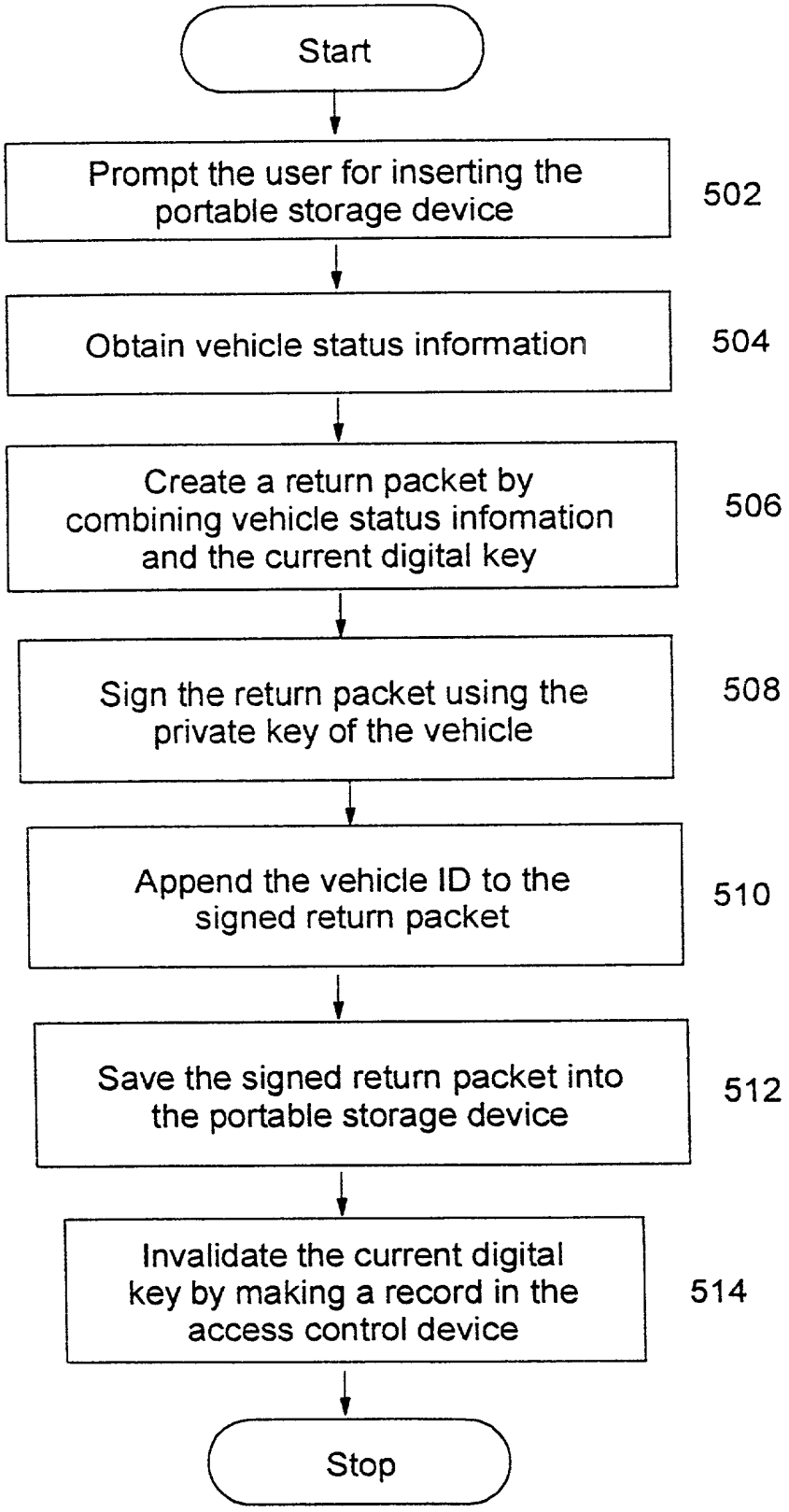

Start
Prompt the user for inserting the portable storage device
502
Obtain vehicle status information
504
Create a return packet by combining vehicle status infomation and the current digital key
506
Sign the return packet using the private key of the vehicle
508
Append the vehicle ID to the signed return packet
510
Save the signed return packet into the portable storage device
512
Invalidate the current digital key by making a record in the access control device
514
Stop

Figure 5

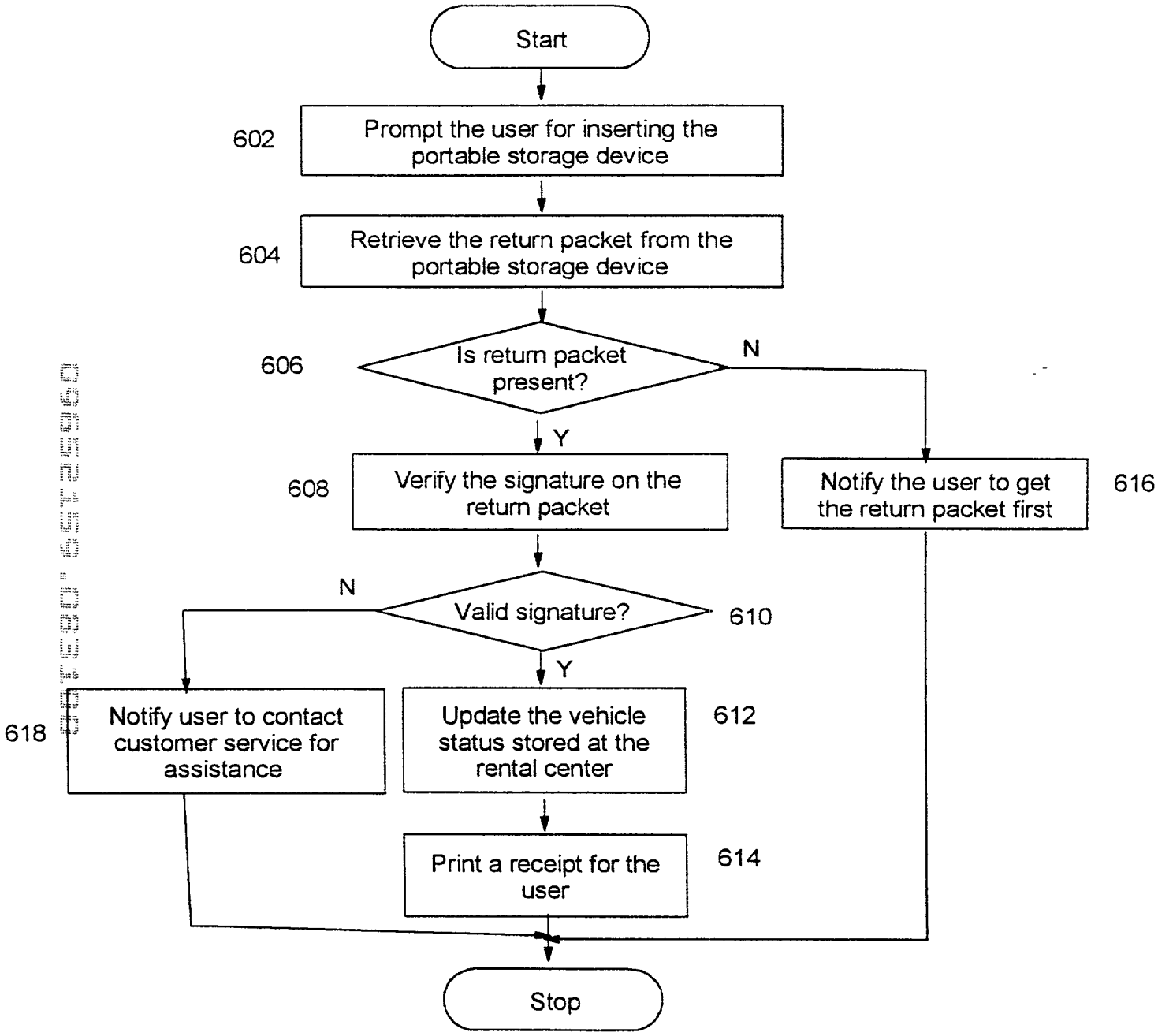

Start
602
Prompt the user for inserting the portable storage device
604
Retrieve the return packet from the portable storage device
606
Is return packet present?
N
Y
608
Verify the signature on the return packet
Notify the user to get the return packet first
616
N
Valid signature?
610
Y
618
Notify user to contact customer service for assistance
Update the vehicle status stored at the rental center
612
Print a receipt for the user
614
Stop

Figure 6

Docket No.: YOR9-2000-0385US1

Application for United States Patent
Declaration and Power of Attorney

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled ACCESS CONTROL FOR RENTAL CARS the specification of which:

(check one)
- ☒ is attached hereto
- ☐ was filed on _____ as Application Serial No. _____ and was amended on _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).*

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	yes	no
(Number)	(Country)	(Day/Month/Year Filed)	yes	no

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.) (Filing Date) (Status: patented, pending, abandoned)

Power of Attorney: As a named inventor, I hereby appoint Manny W. Schecter, Reg. No. 31,722, Terry J. Ilardi, Reg. No. 29,936, Stephen C. Kaufman, Reg. No. 29,551, Louis J. Percello, Reg. No. 33,206, Jay P. Sbrollini, Reg. No. 36,266, Robert M. Trepp, Reg. No. 25,933, Daniel P. Morris, Reg. No. 32,053, Wayne L. Ellenbogen, Reg. No. 43,602, Douglas W. Cameron, Reg. No. 31,596, David M. Shofi, Reg. No. 39,835, Christopher A. Hughes, Reg. No. 26,914, Edward A. Pennington, Reg. No. 32,588, John E. Hoel, Reg. No. 26,279, Joseph C. Redmond, Jr., Reg. No 18,753, C. Lamont Whitham, Reg. No. 22,424, Marshall M. Curtis, Reg. No. 33,138, Michael E. Whitham, Reg. No. 32,635 and Joseph M. Martinez de Andino, Reg. No. 37,178, as attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. All correspondence should be directed to McGuireWoods, LLP, 1750 Tysons Boulevard, Suite 1800, Tysons Corner, McLean, Virginia 22102-3915. Phone calls should be directed to McGuireWoods, LLP, at 703/712-500.

Docket No.: YOR9-2000-0385US1

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

(1) Inventor: Te-Kai Liu

Signature: _____ Date: 8/25/2000

Residence: 23 Pine View Road, Mount Kisco, NY 10549

Citizenship: Taiwan

Post Office Address: Same as Residence

(2) Inventor: Michael C. Greenwood

Signature: _____ Date: _____

Residence: 8 Alana Lane, Holmes, NY 12531

Citizenship: United States of America

Post Office Address: Same as Residence

Title 37, Code of Federal Regulations, §1.56(a):

(a) A duty of candor and good faith toward the Patent and Trademark Office rests on the inventor, on each attorney or agent who prepares or prosecutes the application and on every other individual who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application. All such individuals have a duty to disclose to the Office information they are aware of which is material to the examination of the application. Such information is material where there is substantial likelihood that a reasonable examiner would consider it important in deciding whether to allow the application to issue as a patent. The duty is commensurate with the degree of involvement in the preparation or prosecution of the application.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and (1) it establishes, by itself or in combination with other information, a prima facie case of unpatentability; or (2) it refutes, or is inconsistent with, a position the applicant takes in: (i) opposing an argument of unpatentability relied on by the Office, or (ii) asserting an argument of patentability.

Docket No.: YOR9-2000-0385US1

Application for United States Patent
Declaration and Power of Attorney

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **ACCESS CONTROL FOR RENTAL CARS** the specification of which:

(check one)

☒ is attached hereto

☐ was filed on_____ as
Application Serial No. _____
and was amended on _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1 56(a).*

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	yes	no
(Number)	(Country)	(Day/Month/Year Filed)	yes	no

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status: patented, pending, abandoned)

Power of Attorney: As a named inventor, I hereby appoint Manny W. Schecter, Reg. No. 31,722, Terry J. Ilardi, Reg. No. 29,936, Stephen C. Kaufman, Reg. No. 29,551, Louis J. Percello, Reg. No. 33,206, Jay P. Sbrollini, Reg. No. 36,266, Robert M. Trepp, Reg. No. 25,933, Daniel P. Morris, Reg. No. 32,053, Wayne L. Ellenbogen, Reg. No. 43,602, Douglas W. Cameron, Reg. No. 31,596, David M. Shofi, Reg. No. 39,835, Christopher A. Hughes, Reg. No. 26,914, Edward A. Pennington, Reg. No. 32,588, John E. Hoel, Reg. No. 26,279, Joseph C Redmond, Jr., Reg. No 18,753, C. Lamont Whitham, Reg. No. 22,424, Marshall M. Curtis, Reg. No. 33,138, Michael E. Whitham, Reg. No. 32,635 and Joseph M. Martinez de Andino, Reg. No. 37,178, as attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. All correspondence should be directed to McGuireWoods, LLP, 1750 Tysons Boulevard, Suite 1800, Tysons Corner, McLean, Virginia 22102-3915. Phone calls should be directed to McGuireWoods, LLP, at 703/712-500.

Docket No.: YOR9-2000-0385US1

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

(1) Inventor: Te-Kai Liu

Signature: _____ Date: _____

Residence: 23 Pine View Road, Mount Kisco, NY 10549

Citizenship: Taiwan

Post Office Address: Same as Residence

(2) Inventor: Michael C. Greenwood

Signature: _____ Date: 8/28/2000

Residence: 8 Alana Lane, Holmes, NY 12531

Citizenship: United States of America

Post Office Address: Same as Residence

*Title 37, Code of Federal Regulations, §1.56(a):
(a) A duty of candor and good faith toward the Patent and Trademark Office rests on the inventor, on each attorney or agent who prepares or prosecutes the application and on every other individual who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application. All such individuals have a duty to disclose to the Office information they are aware of which is material to the examination of the application. Such information is material where there is substantial likelihood that a reasonable examiner would consider it important in deciding whether to allow the application to issue as a patent. The duty is commensurate with the degree of involvement in the preparation or prosecution of the application.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and (1) it establishes, by itself or in combination with other information, a prima facie case of unpatentability; or (2) it refutes, or is inconsistent with, a position the applicant takes in: (i) opposing an argument of unpatentability relied on by the Office, or (ii) asserting an argument of patentability.